



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------------------|-------------|----------------------|---------------------|------------------|
| 10/575,416 | 10/19/2006 | Stephan J. Engberg | 606-128-PCT-PA | 9357 |
| 22145 | 7590 | 07/18/2007 | EXAMINER | |
| KLEIN, O'NEILL & SINGH, LLP | | | LE, CANH | |
| 43 CORPORATE PARK | | | ART UNIT | PAPER NUMBER |
| SUITE 204 | | | 2139 | |
| IRVINE, CA 92606 | | | | |

| | |
|------------|---------------|
| MAIL DATE | DELIVERY MODE |
| 07/18/2007 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

| | | |
|------------------------------|-----------------|---------------------|
| Office Action Summary | Application No. | Applicant(s) |
| | 10/575,416 | ENGBERG, STEPHAN J. |
| | Examiner | Art Unit |
| | Canh Le | 2139 |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 10 April 2006.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-18 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-18 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 10 April 2006 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

| | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____. _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This Office Action is in response to the application filed on 04/10/2006. Claims 1-18 are pending and have been examined.

Information Disclosure Statement

The references cited in the application should be included in the IDS to be considered.

Specification

The specification is objected for not disclosing figures 1-2, 9, 12, and 14-17 of the drawing.

The disclosure is objected to because of the following informalities: There is an abbreviation that does not spell out the expression the first time it is used. The abbreviation should spell out the expression the first time it is used and then be followed by parentheses. The abbreviation can be found in the specification such as "MAD-device" in paragraph [0224]. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-2, 5-7, 9-10, 11-12, and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites, " a first legal entity" and "a second legal entity" where its meaning are unclear. This ambiguity renders claim 1 indefinites.

Claims 5 and 15 recite, " PSTN, a GSM network, a CDMA network, and UTMS network" where its meaning are unclear. This ambiguity renders claim 5 indefinites.

Claim 7 recites, "third legal entity" where its meaning is unclear. This ambiguity renders claim 7 indefinites.

Claim 11 recites, "specific identification information" where its meaning is unclear. This ambiguity renders claim 11 indefinites.

Claim 12 recites, "fourth legal entity" where its meaning is unclear. This ambiguity renders claim 12 indefinites.

Claim 2 recites the limitation "the group consisting " in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 6 recites the limitation "the authenticated holder " in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 9 recites the limitation "the context risk " in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "the holder " in line 3. There is insufficient antecedent basis for this limitation in the claim.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 6, 13-14, and 16 are rejected under 35 U.S.C. 102(b) as being anticipated by Herz et al. (5,754,938).

As per claim 1:

Herz teaches a method of establishing a communication path from a first legal entity in

a data communication network, comprising the steps of:

(a) providing at least one private reference point comprised in said data communication network [Col. 32, lines 3-65; **"our method solves the above problems by combining the pseudonym granting and credential transfer methods taught by D. Chaum and J. H. Evertse, in the paper titled "A secure and privacy-protecting protocol for transmitting personal information between organizations," with the implementation of a set of one or more proxy servers distributed throughout the network N. Proxy servers may be the same or different"; a proxy server is equivalent to private reference point];**

(b) establishing a communication path from said first legal entity to said private reference point [Col. 31, lines 48-55, **"A pseudonym is an artifact that allows a service provider to communicate with users and build and accumulate records of their preferences over time, while at the same time remaining ignorant of the**

users' true identities, so that users can keep their purchases or preferences private"; a user's true identity is equivalent to a first legal entity].

(c) verifying the authentication of said first legal entity relative to said private reference point from said first legal entity [Col. 30, line 39-43; Col. 37, lines 48-53; **"The proxy server may verify those credentials and make appropriate modifications to the user's profile as required by these credentials such as recording the user's new demographic status as an adult. It may also store those credentials, so that it can present them to service providers on the user's behalf"**], and

(d) establishing communication from said private reference point to a second legal entity through said data communication network without disclosing the identity of said first legal entity [Col. 31, line 57 to Col. 32, line 2; **"service provider may require proof that the purchaser has sufficient funds on deposit at his/her bank, which might possibly not be on a network, before agreeing to transact business with that user. The user, therefore, must provide the service provider with proof of funds (a credential) from the bank, while still not disclosing the user's true identity to the service provider"; a second legal entity is equivalent to a service provider]**.

As per claim 2:

Herz further teaches the method according to claim 1, further comprising a preliminary step of authenticating said first legal entity by registering data selected from the group consisting of biometrics, a signature, a code and any combinations thereof and comparing the registered data with correspondingly stored data [Col. 31, lines 53-63; **“A second and equally important requirement of a pseudonym system is that it provide for digital credentials, which are used to guarantee that the user represented by a particular pseudonym has certain properties. These credentials may be granted on the basis of result of activities and transactions conducted by means of the system for customized electronic identification of desirable objects, or on the basis of other activities and transactions conducted on the network N of the present system, on the basis of users' activities outside of network N”**].

As per claim 3:

Herz further teaches the method according to claim 1, said first legal entity being an identity device [Col. 30, lines 39-43; Col. 31, lines 48-55, **“A pseudonym is an artifact that allows a service provider to communicate with users and build and accumulate records of their preferences over time, while at the same time remaining ignorant of the users' true identities, so that users can keep their purchases or preferences private”; a user's true identity (e.g. smart card) is equivalent to an identity device**].

As per claim 6:

Herz further teaches method according to claim 1, said private reference point being addressable by the authenticated holder of said first legal entity from a computer communicating with said data communication network [Col. 32, lines 3-65; “our method solves the above problems by combining the pseudonym granting and credential transfer methods taught by D. Chaum and J. H. Evertse, in the paper titled "A secure and privacy-protecting protocol for transmitting personal information between organizations," with the implementation of a set of one or more proxy servers distributed throughout the network N. Proxy servers may be the same or different”].

Claim 13 is essentially the same as claim 1 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 14 is essentially the same as claim 2 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 16 is essentially the same as claim 3 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim*** rejected under 35 U.S.C. 103(a) as being unpatentable over ***.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 4-5, 7-11, 15, and 17-18 are rejected under 35 U.S.C. 103(a) as being anticipated by Herz et al. (5,754,938) in view of Engberg et al. ("Privacy Authentication – persistent non-identification in Ubiquitous environments", August 18, 2002, pages 1-6)

As per claim 4:

Herz does not explicitly teach "first legal entity comprises a card including encrypted data, said method further comprising: said first legal entity receiving an encrypted key from said private reference point, decrypting said encrypted key using a second stored key, and decrypting said encrypted data using said key".

However, Engberg teaches the method according to claim 1, wherein said first legal entity comprises a card including encrypted data, said method further comprising:

(a) said first legal entity receiving an encrypted key from said private reference

point [pg. 3; “Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc”].

(b) decrypting said encrypted key using a second stored key [pg. 3; “Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc”], and

(c) decrypting said encrypted data using said key [pg. 3; “Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc”].

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Herz of the invention by including the step of Engberg because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure [pg. 2, 5th paragraph; Enberg].

As per claim 5:

Engberg further teaches the method according to claim 1, said communication network being selected from the group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a PSTN, a GSM network, a CDMA network, a UMTS network and any

combinations thereof [pg. 1; “**In ubiquitous computing macro (long-distance GSM, UMTS etc.) wireless communication is integrating with micro (local Bluetooth, infrared etc.) wireless communication as part of users general identity end environment management”**].

As per claim 7:

Engberg further teaches the method according to claim 1, further comprising said first legal entity allowing or blocking access to said private reference point by a third legal entity [pg. 2, “**The outcome is a setup in which a PAD device can establish an authenticated wireless IP-session with the normal subscription telecom provider (STP) without the STP having any persistent device or user identifier to link one session with a PAD-device to the next and still have traceability in case the PAD-device user is involved in any criminal activity”**].

As per claim 8:

Engberg further teaches the method according to claim 7, wherein said third legal entity is a party selected from the group consisting of a third party and said first legal entity [pg. 2, “**The outcome is a setup in which a PAD device can establish an authenticated wireless IP-session with the normal subscription telecom provider (STP) without the STP having any persistent device or user identifier to link one session with a PAD-device to the next and still have traceability in case the PAD-device user is involved in any criminal activity”**].

As per claim 9:

Engberg further teaches method according to claim 1, wherein said communication involves creating and negotiating an accountability path for this otherwise anonymous transaction dynamically adapted to the context risk profile [pg. 3, **"Key to Privacy Authentication is the existence of Privacy Accountability. The various properties of Privacy Accountability including how it could be established are not discussed in this paper even though it is highly relevant. We assume the existence of a data component incorporating either identifying (a signature, a verified biometrics) or otherwise linking information together with a verified link to the public key of pseudonym. The data component is encrypted using multiple layers in such a way that it is not providing linkability by its existence and only through a series of steps including multiple trusted parts lead to disclosure of identity or other linking information ... Relevant for this paper is the consideration that possession of a data component providing such properties is not in itself identifying as identity is not readily accessible nor is it clearly anonymous as linkability exists. Privacy Accountability is structurally different from an Identity Escrow setup as in a PKI Certificate Authority as the unit in possession of the data component are only trusted to keep the data component in hiding until the disclosure process - for any reason – is required to initiate"].**

As per claim 10:

Same discussion as claim 9.

As per claim 11:

Engberg further teaches the method according to claim 1, wherein said specific identification information is selected from the group consisting of at least one of biometrics, name, digital signature, and a code [pg. 3, **"We assume the existence of a data component incorporating either identifying (a signature, a verified biometrics) or otherwise linking information together with a verified link to the public key of pseudonym"**].

Claim 15 is essentially the same as claim 5 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 17 is essentially the same as claim 4 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 18 is essentially the same as claim 10 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 12 is rejected under 35 U.S.C. 103(a) as being anticipated by Herz et al. (5,754,938) and Engberg et al. ("Privacy Authentication – persistent non-identification in

Ubiquitous environments", August 18, 2002, pages 1-6) in view of Bushboon (US 2006/0155993 A1).

As per claim 12:

Herz further teaches:

establishing communication from said second legal entity to said service provider [Col. 31-32; proxy server is equivalent to identity provider].

providing a fifth legal entity, constituted by a financial institution [Col. 32, lines 1-2; funds (a credential) from the bank].

Engberg further teaches:

said fourth legal entity responding to said information by transmitting an payment accept to said identity provider [pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"],

said identity provider transmitting payment accept to said service provider [pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"], and

said service provider transmitting payment accept to said second legal entity

[pg. 5; “The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit”].

Herz and Engberg do not explicitly teach an identity provider.

However, Bushboon teaches:

providing an identity provider and a service provider **[par. [0024]; a communication between service provider and identity provider].**
establishing communication from said service provider to said identity provider **[par. [0024]; a communication between service provider and identity provider].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Herz and Engberg of the invention by including the step of Bushboon because it would provide solutions for privacy and data protection problems **[par. [0023], Bushboon].**

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 5521980 A to BRANDS, S A;

US 5754939 A to Herz; Frederick S. M. et al.;

US 20040010713 A1 to Vollbrecht, John R. et al.;

US 7043760 B2 Holtzman; David et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
July 12, 2007



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100